Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. – 21. (canceled)

22. (new) A server comprising:

a storage device which stores identification information of a user terminal and communication capability information of said user terminal; and

a controller connected to said storage device,

wherein said storage device further stores access permission setting values of said identification information and said communication capability information, and vertical relation information indicating a vertical relation between access permission information of said identification information and access permission information of said communication capability information, the vertical relation information indicating that the access permission information of said identification information is in a higher level than that of the access permission information of said communication capability information, and

wherein when the access permission setting value of said communication capability information is changed from a not permitted state to a permitted state, said controller sets the access permission setting value of said identification information to a permitted state, and when the access permission setting value of said identification information is changed from a permitted state to a not permitted state,

said controller sets the access permission setting value of said communication capability information to a not permitted state.

23. (new) The server according to claim 22, wherein

said access permission setting values include the values for an open operation, a read operation and a write operation of information to be accessed.

24. (new) The server according to claim 23, wherein

said access permission setting values for said open, read and write operations have hierarchical levels, the level of the access permission setting values of said open operation being higher than that of said read operation, and the level of the access permission setting values of said read operation being higher than that of said write operation, and

when the access permission setting values of a lower level operation are changed from a not permitted state to a permitted state, said controller sets the access permission setting values of a higher level operation relative to the lower level operation being changed, to a permitted state; and when the access permission setting values of a higher level operation are changed from a permitted state to a not permitted state, said controller sets the access permission setting values of a lower level operation relative to the higher level operation being changed, to a not permitted state.